Chapter 4
Micro-Frauds:
Virtual Robberies, Stings and Scams in the Information Age

David. S. Wall
University of Durham, UK

ABSTRACT

During the past two decades, network technologies have shaped just about every aspect of our lives, not least the ways by which we are now victimized. From the criminal's point of view, networked technologies are a gift. The technologies act as a force multiplier of grand proportions, providing individual criminals with personal access to an entirely new field of 'distanciated' victims across a global span. So effective is this multiplier effect, there is no longer the compulsion to commit highly visible and risky multi-million-dollar robberies when new technologies enable offenders to commit multi-million-dollar thefts from the comfort of their own home, with a relatively high yield and little risk to themselves. From a Criminological perspective, network technologies have effectively democratized fraud. Once a 'crime of the powerful (Sutherland, 1949; Pearce, 1976; Weisburd, et al., 1991; Tombs and Whyte, 2003) that was committed by offenders who abused their privileged position in society, fraud can now be committed by all with access to the internet. This illustration highlights the way that computers can now be used to commit crimes, and this chapter will specifically focus upon the different ways that offenders can use networked computers to assist them in performing deceptions upon individual or corporate victims in to obtain an informational or pecuniary advantage.

INTRODUCTION

A deliberate distinction is made here between *crimes using computers,* such as frauds, *crimes against computers*, where computers themselves are the focus of attack, and *crimes in computers*, where their content is exploited. These latter two groups of cybercrimes are discussed elsewhere (see, for example, Wall, 2007: 45-47, and chs. 4 & 5).

DOI: 10.4018/978-1-61692-805-6.ch004

The most common use of computers for criminal gain is to fraudulently appropriate informational goods, not just money. For the purposes of this discussion, the term 'micro-fraud' is used intentionally, this is because most of the victimizations are not only informational, but also networked and globalised. They also tend to be individually small in impact, but so numerous that they only become significant in their aggregate (Wall, 2007). Conceptually, micro-frauds are those online frauds that are deemed to be too small to be acted upon and which are either written off by victims (typically banks) or not large enough to be investigated by policing agencies. These qualities distinguish the micro-fraud from the larger frauds that also take place online and which tend to capture a disproportionate amount of media attention – even if it is mainly because of their 'infotainment' value (Levi, 2006: 1037). Yet, these larger frauds are relatively small in number when placed against a backdrop of the sheer volume of online transactions. Micro-frauds are the opposite; they are highly numerous and relatively invisible. As a consequence, their *de minimis* quality stimulates a series of interesting criminal justice debates, not the least because micro-frauds tend to be resolved to satisfy private (business or personal) rather than public interests.

The purpose of this chapter is, therefore, to map out online fraud in terms of its distinctive qualities and to outline any changes that have taken place over time. Part one explores the *virtual bank robbery*, in which offenders exploit financial management systems online, mainly banking and billing. Part two looks at the *virtual sting* and the way that offenders use the Internet to exploit system deficiencies to defraud businesses. Part three focuses on the *virtual scam,* defined as the techniques by which individuals are 'socially engineered' into parting with their money. The final part discusses the prevalence of micro-fraud and some of the issues arising for criminal justice systems and agencies.

PART ONE: THE VIRTUAL BANK ROBBERY

As the Internet has become a popular means by which individuals and organizations manage their financial affairs, financial and billing systems have increasingly become exploited as targets for criminal opportunity. Fraudsters have for some time used the Internet to defraud banks, build up false identities, open accounts, and then run them to build up credit ratings to obtain personal loans that are subsequently defaulted upon. Electronic banking is also used to launder money and to turn 'dirty money' into clean money by obscuring its origins through quick transfer from one bank to another and across jurisdictions. Although easy in principal, it is nevertheless quite hard in practice to deceive banking security checks, so offenders will weigh-up the risks of being caught (or prevented) against opportunities. However, "criminals will go to wherever the easiest target is" (Cards International, 2003), so fraudsters will seek out system weaknesses, which tend to lie at the input and output stages. Although not always easy to separate in practice, *input fraud*, or identity theft, is where fraudsters obtain personal or financial information that can give them illegal access to finance [Note: input frauds are discussed elsewhere; see, for example, Wall, 2007; Finch, 2002; Finch & Fafinski, 2010)]. *Output frauds* are where access to credit, usually credit cards, is used to fraudulently obtain goods, services or money.

From the earliest days of e-commerce, online retailers have fallen victim to fraudsters who have obtained their goods by deception, either by supplying false payment details or by using a false address to have goods sent to. During the early days of e-commerce, personal cheques and bank drafts were the focus of online frauds, simply because they were the preferred methods of payment at the time; but they were quickly surpassed by credit cards when online credit card payment facilities became more popular and practical. Although third-party escrowed Internet